REMARKS

The examiner is thanked for the performance of a thorough search and for entering the Applicant's submission filed on November 26, 2004.

Claims 1, 5-7, 9-14, 16, and 21-22 have been amended. Claims 2, 3, 4, 8, 15, 25, and 26 have been cancelled. No claims have been added. Hence, Claims 1, 5-7, 9-14, and 16-24 are pending in the application. Each issue raised in the Office Action mailed March 9, 2005 is addressed hereinafter.

I. INTERVIEW SUMMARY

The Applicants appreciate the courtesy of the Examiner in extending an in-person interview that was held on July 14, 2005 with the Applicant's representative Mr. Christopher Palermo. The Examiner has provided an Interview Summary which appears accurate and is adopted herein. For this reason, the Applicant understands that it is not necessary to provide a separate Summary of Record of Interview at this time.

II. STATUS OF CLAIMS

Claims 1, 5, 7, 9-10, 16-17, and 20-24 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by Garcia, Jr. et al, U.S. Patent No. 6,470,357 ("GARCIA"). Claim 6 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over GARCIA in view of Day, II et al., U.S. Patent No. 5,968,116 ("DAY"). Claims 11-14 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over GARCIA in view of Baum et al., U.S. Patent No. 6,400,707 ("BAUM"). Claims 18-19 have been rejected under 35 U.S.C. § 103(a) as allegedly

unpatentable over GARCIA in view of Nessett et al., U.S. Patent No. 5,968,176 ("NESSETT"). The rejections are respectfully traversed.

III. REJECTIONS BASED ON THE CITED ART

A. OVERVIEW

As discussed in the Interview, the claims in the present application differ from the cited references in a fundamental way. In the claims, directory enabling elements are hosted within a network element that routes or switches packets at OSI Layers 2 or 3. In contrast, in GARCIA a directory service is implemented at an application layer, namely in a TMN network that is logically situated higher than the layers used for packet switching and routing. This difference is illustrated, for example, in ERICSSON, *Understanding Telecommunications, Chapter 8 Network Management, Section A.8.3 Telecommunications management network,* http://www.ericsson.com/support/telecom/part-a/a-8-3.html (hereinafter ERICSSON), which is submitted in the Information Disclosure Statement filed herewith. In ERICSSON, Figure A.8.11 at page 3 of 8 shows a telecommunications network with network elements at a lower layer and a TMN at a higher layer. The claims of the present application are concerned with network elements as shown in the lower part of the Figure, and not with a TMN or its components as shown in the upper part of the Figure.

Further, the claims of the present application feature a locator service that enables an application program to locate servers that provide directory services. GARCIA has no such locator service. Solely for purposes of clarifying the claimed subject matter, amended Claim 1 also recites that the directory service may be an LDAP directory or an

X.500 directory; Applicants believe that this subject matter was inherent in the original claims, but have added it for clarification and not to overcome prior art.

B. <u>GARCIA does not disclose the "locator service" features of Claims 1, 5-7, 9-10, 17, and 21-22</u>

Independent Claims 21 and 22 include the feature of "**a locator service** coupled to the directory enabling element and **configured enable the application programs to locate servers that provide the directory services in the network**." Independent Claim 1, and all dependent claims that depend from Claim 1 (Claims 5-7 and 9-10), include a similar feature. Claim 17 also recites a similar feature, "**locating a nearest directory server** and binding the application program to the nearest directory server that is located." GARCIA does not describe, teach, or suggest, the claimed locator service features.

The Office Action asserts that GARCIA describes a locator service feature in col. 7, lines 5-10. This is incorrect. In col. 7, lines 1-10, GARCIA states:

> **The following example operations illustrate some of the functions of the communication system 400. The first scenarios includes a user application retrieving the routing information for a message the user application is about to transmit.** The User Application 408 initializes and connects to the EDS Process 302 through the EDS API 410. Then, a copy of the EDS database 304 is loaded in the local directory services database 412. When the User Application 408 needs to transmit a message, the User Application 408 accesses the Local EDS Database 412 through the EDS API 410 and retrieves the desired routing information for the message. (Emphasis added)

This merely describes how a user application retrieves the routing information for a message the user application is about to transmit. However, nothing in this passage suggests that the user application includes or utilizes a feature that is capable of **locating** the EDS process 302 or EDS database 304 on the network. The user application is aware

of where the EDS process 302 is located and simply connects to it. In contrast, the locator service of Claim 1 is configured to locate servers that provide directory services on the network.

The Office Action also asserts that the locating feature of Claim 17 is described in col. 5, lines 14-20. This is incorrect. In col. 5, lines 14-20, GARCIA states:

> In FIG. 2, the TMN system 200 illustrates a requester server 202 and a responder server 204 communicating using the TMN 100 system of FIG. 1. The requester server 202 and the responder server 204 each include at least one application entity 206 and 208 respectively, a message routing 120, a EDS API 122, and an association control 124

Thus, this passage describes the elements of a requester server and a responder server in the context of a Telecommunications Management Network (TMN). However, this passage does not describe that any element of the requester server or the responder server is configured to **locate** a server or process in the TMN network that provides EDS services. In contrast, Claim 17 includes the feature of locating the nearest server that provides directory services on the network.

Since GARCIA does not describe a locator service feature, GARCIA does not anticipate Claims 1, 5-7, 9-10, 17, and 21-22 under 35 U.S.C. § 102(e). Reconsideration and withdrawal of the rejections of Claims 1, 5-7, 9-10, 17, and 21-22 are respectfully requested.

C. <u>GARCIA does not disclose the "bind service" features of Claims 5, 10, 12, 14, and 16-20</u>

Claims 5 and 10 include the feature of "**a bind service in the directory enabling element** and **coupled to a security protocol** and **configured to bind an external application program to the security protocol**." Claims 12 and 14 include a similar "bind service" feature. Independent claim 16, and all dependent claims that depend from

Claim 16 (Claims 17-20), recite "**binding an application program to a security protocol**". Thus, Claims 5, 10, 12, 14, and 16-20 include a bind service feature, in which a bind service is coupled to a security protocol and is configured to bind an application program to a security protocol. GARCIA does not describe any such feature.

The Office Action asserts that the Common Management Information Protocol (CMIP) described in GARCIA corresponds to a security protocol as featured in Claims 5, 10, 12, 14, and 16-20. The Office Action further asserts that the claimed bind service features of Claims 5, 10, 12, 14, and 16-20 are described in col. 2, lines 43-47, col. 3, lines 11-30, and col. 3, lines 55-57 of GARCIA. This is incorrect.

CMIP is a widely known protocol that defines an information exchange mechanism for exchanging information objects that are stored in a Management Information Base (MIB). Thus, CMIP cannot be considered to be equivalent to the security protocol featured in Claims 5, 10, 12, 14, and 16-20.

Further, the passages in GARCIA cited by the Office Action do not describe the bind service of Claims 5,10, 12, 14, and 16-20. In col. 2, lines 43-47, GARCIA states:

> Also, an object of the invention is to **allow TMN agent applications and manager applications to send and receive CMIP messages to and from a dispatcher application**. The dispatch application routes the CMIP request using the information in the Enhanced Directory Services. (Emphasis added.)

Thus, this passage describes TMN applications that exchange information with a dispatcher application by using CMIP messages. Nothing in this passage teaches, suggests, or describes that the CMIP protocol is a security protocol, or that the TMN applications are bound in any manner to this protocol. The TMN applications simply use CMIP messages to exchange information with a dispatcher application, and the Applicant

finds nothing in this functionality which suggests that the TMN application are somehow bound to the dispatcher or to the CMIP protocol.

In col. 3, lines 11-33, GARCIA states:

> In the TMN network management framework within the open system interconnection ("OSI") protocol, **an agent, also called "TMN agent" can make management information available to managers**, also called "TMN managers." **Thus, TMN agents offer client applications an open CMIP interface. The TMN agent maintains its management information in a Management Information Base ("MIB").**
>
> In a telecommunications management network ("TMN") system, such as IBM's Telecommunications Management Network Environment ("TMNE"), **messages are routed between applications, also known as application entities. For example, an application may need to send a Common Management Information Protocol ("CMIP") request to the application managing a particular resource.** However, the requesting application may not know which application is managing that resource.
>
> **The requesting application uses an enhanced directory services ("EDS") to route the message and determine the characteristics of the requested application.** Thus, in the current system, the application need not maintain a master list of which application is the appropriate recipient of each message and the routing information and characteristics for that application. (Emphasis added.)

Thus, this passage describes the mechanism of sending messages from one application entity in a TMN network to another. In particular, in a TMN network **messages are sent from a requesting application to a requested application** in the following manner: (1) the requesting application retrieves information from an EDS service, which information is used by the requesting application to send a CMIP message to the appropriate requested application; and (2) based on the information retrieved from the EDS service, the requesting application sends its CMIP message to the requested application. Thus, "the [requesting] application need not maintain a master list of which application is the appropriate recipient of each message and the routing information and characteristics for that application." (GARCIA, col. 3, lines 30-33.)

Nothing in the above passage suggests that the CMIP messages are used for any security-related purposes, or that any binding between the requesting application and the requested application occurs over the CMIP protocol. On the contrary, the passage makes it abundantly clear that the CMIP protocol is used by the requesting application to send a message to the requested application to request a particular resource, and not for any security-related purposes. The passage is silent as to any bindings over the CMIP protocol between the requesting application, the requested application, and/or the EDS service. Indeed, the passage even teaches away from the claims by touting the advantage of not having a master list or anything else that binds applications.

In col. 3, lines 55-57, GARCIA states that "[t]he dispatcher process 310 uses an EDS API to look up routing information and for additional information concerning CMIP peers which will receive CMIP messages." Nothing in this passage even remotely suggests, teaches or describes that the CMIP protocol is used for security-related purposes or that the dispatcher process is bound to the CMIP protocol.

For these reasons, GARCIA does not describe the bind service of Claims 5, 10, 12, 14, 16, 17, and 20. Furthermore, in rejecting Claims 18 and 19, the Office Action relies explicitly on GARCIA, and not on NESSETT, to support prior disclosure of the bind service. Since GARCIA does not describe any bind service, a combination of GARCIA with NESSETT necessarily fails to teach all of the features of Claims 18 and 19. Therefore, reconsideration and withdrawal of the rejections of Claims 5, 10, 12, 14, and 16-20 are respectfully requested.

D. <u>GARCIA does not disclose the "event service" features of Claims 7, 10, 12, 14, and 16-20</u>

Claims 7, 10, 12 and 14 recite "**an event service** coupled to the directory enabling element and **configured to receive registration of an event and an associated responsive action from an application program**, notify the application program when the event occurs, and **execute the associated responsive action in response thereto**." Independent 16, and all dependent claims that depend from Claim 16 (Claims 17-20), include similar event service features by reciting "**creating an event and an associated responsive action that are associated with the application program**; **in response to occurrence of the event, executing the responsive action**, ..." Thus, Claims 7, 10, 12, 14, and 16-20 recite an event service configured to receive registration of an event and an associated responsive action from an application program, and to execute the responsive action in response to the occurrence of the event.

GARCIA does not describe any such feature. The Office Action asserts that the event service features of Claims 7, 10, 12, 14, and 16-20 are described in col. 4, lines 25-28, col. 6, lines 20-27, and col. 6, lines 56-60 of GARCIA. This is incorrect. In col. 4, lines 25-38, GARCIA states:

> The TMN 100 is designed to be a run-time environment for TMN communication utilizing improved associations control 124, message routing 120, enhanced directory services ("EDS") application program interface ("API") 122; and local EDS database 123, also called local directory services database. An application, for example an agent object 110 or a manager 112, communicates with another application utilizing the TMN 100 environment. Applications communicate directly with application entity representation ("AER") 118 or a session control 114. The AER 118 accesses agent services 116 when appropriate to process service requests. The AER 118 communicates with the message routing 120, which interfaces with the external communication services 126.

This passage describes features and elements of a TMN network, and has nothing to do with registering an event and an associated responsive action, and with executing the

associated responsive action when the event occurs. In col. 6, lines 20-27, GARCIA states:

> By storing requested application's information in a directory services database, requesting applications need not track and monitor requested applications characteristics and routing information. Directory services manages the directory information by writing Registration Files and using the directory tools to add and remove CMIP routing information in directory services.

This passage describes how information about a requested application is stored in a directory services database, and how requesting applications need not track and monitor characteristics and routing information about requested applications. Significantly, nothing in this paragraph suggests that the information about a requested or requesting application is capable of storing in the directory services an event and an associated responsive action. Further, nothing in this passage even suggests, teaches or describes that any responsive action is being executed in response to the occurrence of any event.

In col. 6, lines 56-60, GARCIA states:

> The User Application 408 can act as the CMIP dispatcher daemon, as a CMIP based user application, or an EDS Tool, such as the EDS Tools 418. The User Application 408 can search, delete, add, or modify the EDS database 304.

This passage describes the different functionalities that a user application can perform, but does not describe, teach, or suggest, that the user application is capable of registering an event and an associated responsive action in the EDS database. Further, nothing in this passage indicates that an associated responsive action may be executed in response to the occurrence of the event.

The Office Action also asserts that executing the responsive action in Claims 16-20 is described in col. 5, lines 20-45 and col. 7, lines 50-57 of GARCIA. This is incorrect. In col. 5, lines 20-45, GARCIA states:

> In FIG. 3, a configuration is shown with a User Environment 308, also called an application server, a Directory Services Server Environment 300, and a Directory Services Update Application 306. The directory services server environment 300 includes a EDS process 302, also known as a "directory services daemon," and an EDS database 304. The directory services process 302 communicates with the directory services update application 306 and the EDS API 122. The EDS API 112 accesses the Local EDS Database 123.
>
> **The EDS process 302 receives messages from Directory Services Update Applications 306 that indicate that the EDS database 304 was changed by a Directory services Update Application 306. The EDS process 302 then sends a message through the EDS API 122, called a directory services update notice, to the other application entities 206 that use that EDS database (registered applications), notifying them of the changes.** The EDS API 122 provides the routing information to the requesting application or to a dispatcher process 310 that routes the message between requesting and requested applications. If a dispatcher process 310 is used, the applications need not be provided with the routing information.
>
> The EDS Process 302 can be a daemon. A daemon is UNIX process that provides services to user applications and utility applications. That is, it provides low level functions and is accessed through higher level processes. (Emphasis added.)

Thus, this passage describes that one or more application entities may be registered to receive notifications when a directory services update application, such as application 306 in FIG. 3 of GARCIA, changes the EDS database. Significantly, however, this passage does not describe that **changing the EDS database** is created as an event by an application entity, or that it is associated with a responsive action. Furthermore, this passage clearly indicates that **what is registered in the EDS database are the application entities themselves**, and not any events and any responsive actions that are associated with the events. This passage cannot correspond to the claimed feature of executing a responsive action in response to the occurrence of an event that is associated with the responsive action. In col. 7, lines 50-57, GARCIA states:

> Environments, such as User Environment A 402, User Environment B 406 and the Directory Services Server Environment 404, are logical grouping of applications, daemons, databases and other structures that need not reside on a single physical computer. For instance, the User Environment A could be distributed across several IBM RISC System 6000 in a cluster or network configuration.

This passage describes that the components of GARCIA's TMN network may be distributed across several different physical computers. However, nothing in this paragraph suggests that any responsive action is executed in response to the occurrence of an event that is associated with the responsive action, as in Claims 16-20.

For these reasons, GARCIA does not describe the event service features of Claims 7, 10, 12, 14, 16, 17, and 20. Furthermore, in rejecting Claims 18 and 19, the Office Action relies explicitly on GARCIA, and not on NESSETT, to support prior disclosure of the event service features. Since GARCIA does not describe any event service feature, the combination of GARCIA with NESSETT necessarily fails to teach all of the features of Claims 18 and 19. Therefore, reconsideration and withdrawal of the rejections of Claims 7, 10, 12, 14, and 16-20 are respectfully requested.

E. <u>GARCIA does not disclose the "policy" features of Claims 9, 16, 17, 18, 19, 20, and 23</u>

Claims 9 includes "**a group policy interface** coupled to the directory enabling element and **configured to receive and update the directory service with one or more definitions of directory services policies that apply to groups of network devices in the network**." The Office Action asserts that this is described in col. 5, lines 20-45 of GARCIA. This is incorrect.

As discussed above for the claimed event service, the passage in col. 5, lines 20-45 of GARCIA describes that one or more application entities may be registered to

receive notifications when a directory services update application, such as application 306 in FIG. 3 of GARCIA, changes the EDS database. However, nothing in this passage describes, teaches, or suggests that the EDS process uses a group policy interface that is configured to receive and update the directory services with one or more definitions of directory services policies. In fact, nothing in the paragraph suggests that the updates to the EDS database include any information that may be even remotely related to definitions of directory services policies that apply to groups of network devices in the network, as featured in Claim 9.

Independent Claim 16, and all dependent claims that depend from Claim 16 (Claims 17-20), include the similar feature of "... **obtaining policy information from the directory service, and converting the policy information into one or more commands** that are executable by the directory-enabled network element." The Office Action asserts that this feature of Claims 16, 17, and 20 is described in col. 5, lines 20-45 and col. 7, lines 50-57 of GARCIA. This is incorrect.

As discussed above, col. 5, lines 20-45 of GARCIA has nothing to do with policy information. Further, as discussed above for the claimed event service, col. 7, lines 50-57 of GARCIA describes that the components of GARCIA's TMN network may be distributed across several different physical computers. However, nothing in this paragraph teaches or describes obtaining policy information from the EDS service, or converting policy information into one or more commands that are executed by any application. In fact, nothing in any passage of GARCIA describes, teaches or suggests that the EDS may be storing any policy information. Therefore, GARCIA does not describe this feature of Claims 16, 17, and 20.

Claims 18 and 19 further include the feature of "**translating the policy information into one or more values...**". The Office Action does not specify where in GARCIA this feature is described or suggested. Furthermore, in rejecting Claims 18 and 19, the Office Action relies explicitly on GARCIA, and not on NESSETT, to support prior disclosure of the "group policy" feature of these claims. Since GARCIA does not describe anything that is even remotely close to obtaining policy information or translating policy information, a combination of GARCIA with NESSETT necessarily fails to teach all features of Claims 18 and 19.

Claim 23 also recites that "the network element **obtains policy information from the directory services** and updates the directory service." The Office Action asserts that this feature of Claim 23 is described in col. 5, lines 3-25 of GARCIA. This is incorrect. In col. 5, lines 3-28 GARCIA states:

> This approach guarantees high performance because only a single memory block is allocated and freed for each directory service query. This remains true even if the query returns more than one directory service entry. This memory management mechanism guarantees thread-safeness because the EDS API 122 uses the concept of reference pointers to memory blocks. This guarantees that the contents of static data present in a directory entry are returned to the user and not lost, even if the local EDS database 123 is reloaded with the new directory contents.
>
> In FIG. 2, the TMN system 200 illustrates a requester server 202 and a responder server 204 communicating using the TMN 100 system of FIG. 1. The requester server 202 and the responder server 204 each include at least one application entity 206 and 208 respectively, a message routing 120, a EDS API 122, and an association control 124.
>
> In FIG. 3, a configuration is shown with a User Environment 308, also called an application server, a Directory Services Server Environment 300, and a Directory Services Update Application 306. The directory services server environment 300 includes a EDS process 302, also known as a "directory services daemon," and an EDS database 304. The directory services process 302 communicates with the directory services update

> application 306 and the EDS API 122. The EDS API 112 accesses the Local EDS Database 123.

The Applicant cannot determine anything in this passage that corresponds to policy information that is stored in the EDS database. Further, nothing in this passage that even remotely corresponds to the claimed feature of a network element obtaining policy information from the directory services. Thus, GARCIA does not describe the above-noted feature of Claim 23.

For the above reasons, GARCIA does not describe all the features of Claims 9, 16, 17, 18, 19, 20, and 23. Therefore, reconsideration and withdrawal of the rejections of Claims 9, 16, 17, 18, 19, 20, and 23 are respectfully requested.

F. <u>GARCIA does not disclose the feature of Claims 11 and 12 of a directory–enabled packet router that is capable of manipulating packets at OSI Layer 2 or 3</u>

Independent Claim 11 includes a **directory-enabled packet router that is capable of manipulating packets at OSI Layer 2 or 3**. Further, since Claim 12 depends from Claim 11, it includes each and every feature of Claim 11. The Office Action asserts that the feature of a directory-enabled router that is capable of manipulating packets is described in col. 3, lines 11-30 of GARCIA. This is incorrect. In col. 3, lines 11-33, GARCIA states:

> In the TMN network management framework within the open system interconnection ("OSI") protocol, an agent, also called "TMN agent" can make management information available to managers, also called "TMN managers." Thus, TMN agents offer client applications an open CMIP interface. The TMN agent maintains its management information in a Management Information Base ("MIB").
>
> In a telecommunications management network ("TMN") system, such as

> IBM's Telecommunications Management Network Environment ("TMNE"), messages are routed between applications, also known as application entities. **For example, an application may need to send a Common Management Information Protocol ("CMIP") request to the application managing a particular resource.** However, the requesting application may not know which application is managing that resource.
>
> **The requesting application uses an enhanced directory services ("EDS") to route the message and determine the characteristics of the requested application**. Thus, in the current system, the application need not maintain a master list of which application is the appropriate recipient of each message and the routing information and characteristics for that application. (Emphasis added.)

Thus, this passage describes the mechanism of sending messages from one application entity in a TMN network to another. In particular, in a TMN network **messages are sent from a requesting application to a requested application** in the following manner: (1) the requesting application retrieves information from an EDS service, which information is used by the requesting application to send a CMIP message to the appropriate requested application; and (2) based on the information retrieved from the EDS service, the requesting application sends its CMIP message to the requested application. Thus, "the [requesting] application need not maintain a master list of which application is the appropriate recipient of each message and the routing information and characteristics for that application." (GARCIA, col. 3, lines 30-33.)

Nothing in the above passage, however, even remotely suggests that a requesting application receives and routes a CMIP message to the requested application. On the contrary, the above passage makes it clear that the requesting application **originates** the CMIP message. Furthermore, the requested application is described in the above passages as "managing a particular resource" in which the requesting application is interested. Thus, the requested application is the **destination** of any message sent from the requesting application. For this reason, since the above passage at most describes a

point-to-point communication between a requesting application and a requested application, the above passage cannot possibly suggest that any of the requesting or the requested applications is **capable of manipulating packets at OSI Layer 2 or 3**, as featured in Claim 11.

Furthermore, GARCIA does not teach, suggest or describe that the messages exchanged by application entities in GARCIA's TMN network are packets exchanged in a packet-switched network. On the contrary, in col. 4, lines 21-23, and with respect to FIG. 1, GARCIA states that "[t]he elements of the TMN 100 correspond with the elements of the protocol hierarchy 102 to their right". As can be seen in FIG. 1, the protocol hierarchy 102 consists of an application entities layer 104, infrastructure layer 106, and external communication services layer 108. Significantly, however, the messages which GARCIA describes as being exchanged in the TMN network originate from an application entity in the application entities layer and are sent to an application entity in the application entities layer. Thus, the messages being exchanged are application-specific messages that are not packets exchanged in a packet-switched network, such as, for example, IP packets.

Furthermore, even though GARCIA mentions that the TMN system may include a TCP/IP stack 128 (col. 4, lines 38-42), nothing in GARCIA teaches, describes, or even suggests that the TMN system or any component of the TMN system receives and routes any packets. Significantly, GARCIA apparently uses the TCP/IP stack 128 only to communicate with other entities, and nothing suggests that the TCP/IP stack may be used for routing packets in a packet-switched network.

In rejecting Claims 11 and 12, the Office Action relies explicitly on GARCIA, and not on BAUM, to support prior disclosure of the feature of a directory-enabled router that is capable of manipulating packets at OSI Layer 2 or 3. Since GARCIA does not describe anything that corresponds to a router, a combination of GARCIA with BAUM necessarily fails to teach all of the features of Claims 11 and 12. For this reason, Claims 11 and 12 are patentable under 35 U.S.C. § 103(a) over GARCIA in view of BAUM. Therefore, reconsideration and withdrawal of the rejections are respectfully requested.

G. <u>GARCIA does not disclose the feature of Claims 13 and 14 of a directory-enabled data switch that is capable of manipulating packets at OSI Layer 2 or 3</u>

Independent Claim 13 includes the feature of a **directory-enabled data switch that is capable of manipulating packets at OSI Layer 2 or 3**. Further, since Claim 14 depends from Claim 13, it includes each and every feature of Claim 13. The Office Action asserts that the feature of a directory-enabled data switch that is capable of manipulating packets at OSI Layer 2 or 3 is described in col. 3, lines 11-30 of GARCIA. This is incorrect.

As discussed above, nothing in col. 3, lines 11-30 of GARCIA teaches, describes, or suggests that the messages exchanged between application entities in GARCIA's TMN system are packets exchanged in a packet-switched network. Furthermore, nothing in this passage even remotely suggests, let alone teaches or describe, that the messages are manipulated by a data switch that is directory-enabled.

In rejecting Claims 13 and 14, the Office Action relies explicitly on GARCIA, and not on BAUM, to support prior disclosure of the feature of a directory-enabled data

switch that is capable of manipulating packets at OSI Layer 2 or 3. Since, as shown above, GARCIA does not describe anything that corresponds to a data switch, the combination of GARCIA with BAUM necessarily fails to teach all of the features of Claims 13 and 14. For this reason, Claims 13 and 14 are patentable under 35 U.S.C. § 103(a) over GARCIA in view of BAUM. Therefore, reconsideration and withdrawal of the rejections of are respectfully requested.

IV. CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed. Further, for the reasons set forth above, the Applicant respectfully submits that allowance of the pending claims is appropriate. Reconsideration of the present application is respectfully requested in light of the amendments and remarks herein.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a law firms check for the petition for extension of time fee is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: August 8, 2005

Stoycho Draganoff
Stoycho D. Draganoff
Reg. No. 56,181

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1080 ext. 208
Facsimile No.: (408) 414-1076